May 30, 2009 - U.S. Scrambles to Develop Cyber Defenses to Fight Internet Hacking

Pittsburgh Tribune-Review

www.pittsburghlive.com

U.S. scrambles
to develop cyber defenses to fight Internet hacking

By Mike Cronin

TRIBUNE-REVIEW

Saturday, May 30, 2009

Last year, Canadian investigators discovered a malicious software program they call GhostNet. They tracked its start to 2007 and have watched it spread to more than 1,300 computers in at least 103 countries, including the United States.

GhostNet can take over a computer's cameras and microphones to spy on its user. Most of the compromised computers traced by Canadian investigators belong to Tibet-related nongovernmental organizations, but some belong to foreign embassy offices in Washington and New York.

The Canadian investigators believe GhostNet resulted from a Chinese government-sponsored intelligence operation.

"It is too complex to be otherwise," said Rafal Rohozinski, CEO of the SecDev Group in Ottawa,

Canada, and a
member of the team that found GhostNet.

A Chinese embassy spokeswoman in Washington, Wei Xin,
declined to comment on GhostNet specifically.

"China's
position is very clear. We have on several occasions reiterated our resolute policy of opposing and cracking down on cybercrimes, including hacking, according to law," she said.

Aggressive cybertactics by other countries should not be a
surprise, Rohozinski said:

"Cyberspace is a domain where countries without the
same conventional military capabilities as the United States can compete."

Concerns about cyberattacks prompted President Obama on
Friday to announce the creation of a White House position to oversee cybersecurity.

Attacks hard to prevent

Attacks on U.S.
computers, systems and infrastructure from countries including China have become more frequent. U.S.
officials announced this year that hackers penetrated the nation's electrical grid, and a virus infected Pentagon computers.

Cyberattacks pose the greatest threat to the United States
after nuclear war and weapons of mass destruction -- and are increasingly hard to prevent, said Shawn Henry, assistant director of the FBI's cyber division, earlier this year.

Some computer-security specialists say China and Russia outstrip the United States in cyberwarfare offensive and defensive capabilities. And they say the capabilities of terrorist and organized-crime groups also pose dangers to the foundations of American life: communication systems, power grids and the money supply.

When U.S. officials revealed last month that hackers from China, Russia and other countries infiltrated the electrical grid, they said the perpetrators left behind "sleeper" software, according to Kevin G. Coleman, a computer security specialist at The Technolytics Institute in McMurray.

Sleeper software remains dormant until it receives a command to activate and infect an operating system with a virus, take over that system or disable it.

Spokespeople from the Chinese and Russian governments routinely deny their countries are behind such attacks.

U.S. intelligence officials believe China and Russia have developed home-grown secure systems, said Coleman, who consults government agencies and has testified before Congress on computer security issues.

The Pentagon and sensitive government operations use secure systems, but most U.S. operating systems were built commercially or in open-source environments without security as a design priority -- at least until recently, said James Joshi, a University of Pittsburgh professor of information systems and telecommunications.

"One of my research focuses is to develop effective and efficient access control models and frameworks for newly emerging complex operating systems," said Joshi, co-founder and director of Pitt's Laboratory for Education and Research on Security Assured Information Systems.

Last year, hackers accessed computers and used jpeg image files to run malicious codes on Windows systems, said Don Gray, vice president of technical strategy for the Bloomfield office of a Nebraska company, Solutionary. His company provides information security, monitoring and management for about 300 clients, including several federal agencies.

Those codes caused computer crashes, loss of personal information -- credit-card accounts, for example -- and, ultimately, made the infected computers part of the hackers' network, Gray said. Hackers could use the newly corrupted computers to launch attacks on other computers.

Local universities aid effort

Carnegie Mellon University's CyLab, a cybersecurity research and education center, and the university's CERT program are part of the federal government's effort to counter threats from China, Russia and other sources.

The Pentagon established CMU's Software Engineering Institute in 1984 to find ways to safeguard the nation's software. Four years later, at the request of the Defense Advanced Research Projects Agency, the institute established the nation's first computer emergency response team, or CERT, after an Internet worm crippled 10 percent of online computers.

Some of CMU's research develops methods to mathematically identify a visitor to a specific networked computer system as friend or foe and to respond appropriately, said David Brumley, a CMU professor of electrical and computer engineering and computer science.

Brumley said researchers use mathematics because "computers are applied math." Verifying a visitor's identity mathematically enables scientists to show "we didn't make a mistake," he said.

"For example, the U.S. Army could communicate with the U.S. Navy, but the Red Army shouldn't be able to say, 'We're the U.S. Navy.'
"

CMU received an average of $65 million annually from 2004 to 2007 from the Department of Defense and about $12 million annually in 2006-08 from the Department of Homeland Security, said school spokesman Ken Walters.

Cybersecurity research crosses into many disciplines and many projects, and school officials could not provide a separate figure just for that research.

One project includes developing a secure electronic-communication system enabling defense contractors to talk with federal agencies and share information, said Jeffrey Carpenter, technical manager at CERT.

A pilot program consists of about 30 defense contractors. Ultimately, the system could include 8,000 defense contractors, he said.

"This program aims at preventing nonclassified, but sensitive, information from getting out," Carpenter said.

Joshi said he and his colleagues at the University of Pittsburgh are developing methods to keep computers working even if they are under attack.

"That goal is becoming much more crucial: how to cope and maintain communication even when there are ongoing attacks," he said. "We want to maintain as much of system functionality and communication as possible, even when things are not going well."

Pitt received an average of $25 million annually in 2005-08 from the Department of Defense and about $115,000 annually in 2006-08 from the Department of Homeland Security, according to figures provided by school spokesman John Fedele. The government-funded research crosses into many disciplines, and school officials could not provide a separate dollar figure

just for cybersecurity research.

CMU and Pitt do no classified research for the federal government, school officials said.

They receive a small piece of the federal budget. The 2009 fiscal budget contains $515.4 billion for the Defense Department and $50.5 billion for Homeland Security.

China strives for dominance

The Tribune-Review obtained an English-language document prepared by Wuhan University in China that outlined how Chinese computer scientists helped to develop a secure operating system, sometimes referred to as Kylin, for the Chinese government.

The document was posted on a cyberwarfare blog on the professional networking Web site LinkedIn.

Coleman reviewed the document, believed to be written late last year, and said it appears legitimate. Its contents are consistent with documents he read from at least three other sources: China's Ministry of Science and Technology, China's National University of Defense Technology, and a report by Norwich University in Vermont and the U.S. Department of Defense about China's cybertechnology initiatives.

Efforts began in 2000. By 2005, Chinese researchers created a "trusted," or secure, computer chip and computer, according to the document. Chinese computer scientists started researching "trusted" software in 2007, the document said. And last year, Chinese researchers developed the first "trusted" personal digital assistant or PDA.

Cybersecurity experts who have used Kylin say the system is not as impenetrable or widespread as thought, Rohozinski said. It is being used only by researchers.

Still, "China's
stated long-term strategy (is) ... to achieve total world electronic dominance
by 2050," Technolytic's Coleman said. "Think about how far in the
future we plan things: Typically, it's four years, the length of a presidential
administration."

Wei Xin, the Chinese embassy spokeswoman, denied that
hackers from China accessed America's
power grid. She said eight of 10 computers connected to the Internet in China
have been hacked.

Russian capabilities surface

Russia's
cyberwarfare capabilities were revealed last year when cyberattacks from Russia preceded that county's invasion of Georgia,
Coleman said.

Georgian residents could not get news from electronic
sources, and Georgian government and military officials could not communicate
electronically.

Yevgeniy Khorishko, a Russia
embassy spokesman in Washington,
denied that the Russian government launched those cyberattacks. "No one
has ever produced evidence that Russia
attacked any country," he said.

Rohozinski said the government may not have conducted them,
"But Russian officials also did nothing to halt the Russian-based attacks
because they were convenient."

Russian criminals have created the Russian Business Network, which consists of computers infected by malicious software, Gray said. Hackers can pay to use the computers and commit crimes such as identity theft or corporate espionage. "They act like arms dealers, and they're very hard to investigate."

Cyberspace a 'warfighting domain'

Pentagon officials last week said the military plans to create a cybercommand soon.

That announcement followed testimony by Army Lt. Gen. Keith B. Alexander, the National Security Agency director, who told the House Armed Services terrorism subcommittee that the Pentagon is considering a cybercommand.

The Pentagon views cyberspace as a "warfighting domain -- just like air, sea, land and space," said Air Force Lt. Col. Eric Butterbaugh, a Department of Defense spokesman. "Cyberspace is extremely important to our military operations; we must defend it."

Homeland Security officials earlier this month proposed spending $400 million for a National Cybersecurity Division in 2010. The division's budget is $294 million for this fiscal year.

Though Coleman applauded Obama's approach, he said China is expected to have another advantage: It may have the world's largest economy by 2030; the United States could drop to fourth by then, behind Russia and India.

"China's going to be able to spend as much as we spend on our military, and their labor costs are 30 percent of what ours are," he said.

A substantial amount of America's computer components are built outside the United

States, and China is a major supplier.

Last month, Rep. John Murtha, D-Johnstown, chaired a closed-door House Appropriations Defense Subcommittee briefing with the FBI and NSA on the security risks of communication devices such as the BlackBerry.

"The threats we face from cyberattacks are real, and the U.S. is actively developing cybersecurity tools to disrupt and thwart these attacks," Murtha said.

Sens. Olympia Snowe, R-Maine, and Jay Rockefeller, D-W.Va., have introduced a bill to address U.S. vulnerability to cybercrime, global cyberespionage and cyberattacks. It would, for example, require that private-sector networks be as secure as government networks.

Yet some experts fear U.S. officials won't respond effectively until a defining event, such as the Russian satellite launch in 1957 that ignited the space race.

"People didn't perceive it as a threat until they could go outside at night and see that light (from the Sputnik satellite) going across the sky," Gray said.